International Journal of Civil Law and Legal Research

E-ISSN: 2789-8830
P-ISSN: 2789-8822
IJCLLR 2025; 5(1): 13-17
www.civillawjournal.com
Received: 10-10-2024
Accepted: 20-11-2024

Dr. Atika Bano
Associate Professor, Glocal University, Saharanpur, Uttar Pradesh, India

Zainab Khan
Research Scholar, Glocal University, Saharanpur, Uttar Pradesh, India

Correspondence
Dr. Atika Bano
Associate Professor, Glocal University, Saharanpur, Uttar Pradesh, India

Cyber Crime and cyber terrorism in Indian: An analysis

Atika Bano and Zainab Khan

Abstract
Societies are becoming more susceptible to cybercrime as a result of the amazing development of the information society and its reliance on Internet use globally, and especially in India. Because internet is a free-flowing, borderless, and worldwide issue, cybercriminals are not limited by geographic boundaries. Local laws are powerless to stop these crimes; in this situation, India is like a sitting duck. India has signed a number of bilateral agreements to combat cybercrime, including a framework agreement with the US and a cyber agreement with Russia. The recent visit of Indian Prime Minister Mr. Modi to Israel to sign the Indo-Israel Cyber Framework is another attempt by India to simplify its cyberspace. These bilateral agreements are insufficient and ineffectual in addressing cybercrime, and their scope is restricted. India need a multilateral agreement that will address international cooperation in the fight against cybercrimes on a worldwide scale and unify its laws through a unified criminal policy. The convention should aid in the development of strong investigative methods and efficient laws that can promote global cooperation in the fight against cybercrime's One such international multilateral agreement that addresses international cooperation in the fight against cybercrimes on a worldwide scale is the Council of Europe's Budapest Convention on Cybercrime. Although the US and Israel, with whom India has bilateral agreements to combat cybercrime, have joined the Budapest Cybercrime Convention, India should also sign the convention.

Keywords: Cyber, convention, India, cybercrime, council of Europe

Introduction
Cyber Crimes are another class of wrongdoings quickly expanding because of broad utilization of Internet and I.T. empowered administrations. System wrongdoing is one of the quickest developing sorts of criminal behavior, both in the U.S. furthermore, universally. While the Internet joins individuals together more than ever, it likewise gives perpetual occasion to hoodlums looking to abuse the weaknesses of others. There are a few unique kinds of system wrongdoing, a large number of which covers. The following are a couple of the most regularly reported. Phishing (Phishing is the act of sending false messages trying to deceive the beneficiary, generally to acquire cash). The old are especially powerless against these sorts of digital crime. Hacking (Hacking is like computerized intruding). Programmers invade online organizations to illicitly download private data, control capacities and now and again take personalities that can be utilized to deceitfully buy merchandise online. Stalking as well as Harassment - Not a wide range of digital wrongdoing include cash. Some digital crooks utilize the Internet as a cover for other illicit practices like following, badgering and in lesser cases, tormenting. The Information Technology (IT) Act, 2000, determines the demonstrations which are culpable. Since the essential target of this Act is to establish an empowering climate for business utilization of I.T., certain particular exclusions and commissions of lawbreakers while utilizing systems have not been incorporated. A few offenses having bearing on digital field are moreover enlisted under the proper segments of the IPC with the legitimate acknowledgment of Electronic Records and the alterations made in a few segments of the IPC vide IT Act, 2000.

Historical background of Cyber Crime and Cyber Terrorism
It would have been astonishing to hear that the first functional computer was developed in the 1950s for anybody who utilizes microchips and palmtops today. The computer was too expensive to operate and was so big it filled up a whole room. The majority of people were unable to understand how these computers worked; only a select few highly competent persons had direct access to these computers and the data required to run them. Before IBM's

invention of the stand-alone personal computer in 1981, for obvious reasons, computer technology was prohibitively expensive and out of the reach of almost everyone. This helped many realize the advantages of quick data access and manipulation that had previously only been appreciated by a small number of people. At the beginning of the twenty-first century, personal computers began to become more widely available and more reasonably priced in India. In the wake of World War II, the US Department of Defense established the Internet in an effort to build a network that could safely transport data and operate during emergencies or times of war. The World Wide Web, Hypertext, and Transmission Control Protocol/Internet Protocol all developed as the original network, known as ARPANET, grew in popularity globally. With the introduction of the Internet, information both in terms of quantity and quality surged. But at that particular period, no one had anticipated the possibilities that the internet would provide to tech-savvy thieves. India's first internet services were introduced by the state-owned Videsh Sanchar Nigam Limited in 1995. But in 1998, the government ended VSNL's monopoly and let private companies into the market. In terms of internet use, 0.1% of Indians were involved. India is now the country with the second-highest percentage of internet users, behind China, with 33.22% of its people using the internet.

Legal Nature of Cyber Crime Acts

Cybercrime acts might be monetarily determined acts, identified with system content, or against the privacy, honesty and openness of system frameworks. The general danger and danger may change among Governments and organizations. Singular cybercrime exploitation is fundamentally higher than for 'ordinary' wrongdoing structures particularly in nations with lower levels of improvement, featuring a need to fortify counteraction endeavors in these nations. Private area undertakings in Europe report exploitation paces of somewhere in the range of 2 and 16 percent for acts, for example, information break because of interruption or phishing. Criminal instruments of decision for these wrongdoings, for example, botnets, have worldwide reach. More than 1,000,000 one of a kind IP addresses around the world worked as order and control workers for botnets in 2011 Internet substance focused for evacuation by governments incorporates kid sexual entertainment and scorn discourse, yet additionally maligning and government analysis, raising basic freedoms law worries in some cases Some gauges place the absolute worldwide extent of web traffic assessed to encroach copyright at very nearly 24 percent.

Cyber Crime Comparison across the World

The rundown of the most perilous nations for system assaults depends on the statistics of 2012. "China and the U.S. may dominate the features with regards to programmer assaults; however, nations in the creating scene are the most helpless to online attacks... While focusing on purchasers, cyber hoodlums are probably going to go where there are less protections. Developing markets give such a chance, with a large number of new Internet clients consistently and less assets to give to security," the office detailed. Notwithstanding, the U.S. was likewise remembered for the rundown - being placed in nineteenth spot with 45% of individuals who went up against digital attacks a year back. The percentage of people that were seen online back in the platforms were accounted to be of 78% of the US population of US. the authorities such as Internet Fraud Complaint Center to safeguard the people's cyber safety was set up on May 8, 2000. After some time, the name was changed to Internet crime complainant center also known as IC3 as the cases were increasing. Today, theIC3 recognizes a bigger number of grumblings in a lone month than it got in its underlying a half year. Although the authority got many objections for its set up but the centre dedicate its duty to safeguard the people from such crimes.

Cyber Crime and its Classification

a) 4 Significant orders are as per the following:

Crime against a person/individual: These are crimes where the cyber convicts use digital attack against a person or individual jeopardizing the victims. Some of digital wrongdoing against individuals is:

- **Email exaggerating:** This technique is an impersonation of an email header. This infers that the message appears to have gotten from someone or somewhere other than the genuine or genuine source. These systems are regularly used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email right when they feel that the email has been sent by a certified source.
- **Spamming:** Email spam which is commonly called as trash email. It is unsought mass message sent through email. The jobs of spam have gotten notable during the 1990s and it is an issue looked by most email customers now a days. Recipient's email addresses are gotten by spam bots, which are robotized programmers that are used for finding email addresses of their targets. These email ids are recorded safety among the spammers, the email hunting is done with an agenda of procuring as many email id's as possible which makes them reach out to many people.
- **Defaming:** Here the harm that is suffered by the victim through a cyber-platform which the cyber convicts initiated through a network.
- **Internet Relay Chat:** this is a platform where all the agents from around the world can join together and converse with other, sharing their contents with each other. These gatherings are called rooms and are used profusely by cyber criminals to plan their attack. The presence of pedophiles was found in this room, with an objective of harassing small children.

Clarifications for IRC

- To create conversations with people under fake id's and manipulate them into believing them and later putting their victims in difficult situations of coercion or black mailing.
- Pedophiles attacking young children for their pleasure and enjoyment.
- Fraud games in business.
- For the purpose of Phishing: "In such a wrongdoings or deception the attacker endeavors to get s information, for instance, login information or record's information by assuming the presence of a reliable individual or component in various correspondence channels or then again in email. Some other digital violations against individuals incorporates Net shakedown, Hacking, Indecent presentation, Trafficking, Circulation, Posting,

Credit Card, Malicious code, etc The conceivable harm of such a malefaction to an extraordinary individual can scarcely be more prominent."

b) Cyber Crime against property: such wrongdoings fuse ruining of framework s, Intellectual (Copyright, authorized, brand name, etc) Property Crimes. Online trading off, etc Protected development wrongdoing joins:

- Software burglary, copyright infringement and trademark infringement: stealing of copyrights with any approval from officials. The infringement of one's rights on materials such as programming, music and prints etc.

c) Crimes against affiliation such as:

- Making changes or deleting data without the approval of the officials.
- DOS attack
- Assaults through emails.

d) Cyber-attack against the society

- Forgery of documents and signs etc.
- Web hijacking

Legal Framework relating to Cyber Crimes in India

- **Section 65:** Intentionally or knowingly causes another person to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system, or computer network when the law requires that the source code be kept or maintained for the duration that it is in effect.
- **Section 66:** Hacking occurs when someone destroys, erases, or modifies any information included in a computer resource, reduces its value or utility, or otherwise changes it in a way that is harmful to the public with the knowledge or intent to cause unjust loss or damage.
- **Section 66B:** When someone obtains or holds onto a communication device or computer resource that is either known to be stolen or that they have cause to suspect is stolen,
- **Section 66C:** Someone uses someone else's password, digital signature, or other distinctive identity information fraudulently.
- **Section 66D:** If a person cheats someone using a computer resource or communication
- **Section 66E:** If someone takes, sends, or publishes pictures of someone else's intimate areas without that person's knowledge or consent.
- **Section 66F:** Cyberterrorism is committed when someone tries to jeopardize India's unity, integrity, sovereignty, or security by preventing authorized personnel from accessing computer resources, gaining access to secured systems, or introducing contaminants into systems.
- **Section 67:** Any content that is lewd, appealing to the prurient interest, or that has the potential to corrupt and deprave those who are likely to read, see, or hear it—after all pertinent circumstances have been taken into consideration—should be published, transmitted, or caused to be published in electronic form.
- **Section 67A:** If someone posts or distributes pictures of a sexually explicit act or behavior.
- **Section 67B:** If someone takes pictures of a youngster engaging in sexually explicit behavior and publishes or distributes them. if someone coerces a minor into engaging in sexual activity. Anyone under the age of eighteen is considered a child.
- **Section 67C:** Intermediaries, including ISPs, are obligated to keep the necessary records for a certain amount of time. Failure is a crime.
- **Section 68:** IF the Controller determines that a Certifying Authority or any of its employees must take certain actions or stop engaging in certain activities in order to guarantee adherence to the terms of this Act, its rules, or any regulations established thereunder, the Controller may grant the order. Any anyone who disregards any such directive will be found guilty of a crime.
- **Section 70:** By publishing a notice in the Official Gazette, the relevant government can designate any computer, computer system, or computer network as a protected system. Authorization to access protected systems may be granted by the relevant government through a written order. Anyone who tries to gain access to a protected system or secures access to one is breaking the law.
- **Section 71:** If someone obtains a license or digital signature certificate by lying to the Controller or the Certifying Authority or by hiding any important information from them.

Nationals approaches to s Cyber Crimes prevention roles of various institutions

Wrongdoing contravention plan with clear necessities and targets should be set up and government should remember lasting guidelines for its tasks and structure for controlling wrongdoing, and assurance that sensible commitments and objectives exist inside government for the relationship of wrongdoing expectation. Notwithstanding the customary laws, enactment must also consider new ideas and article identified with PC information. Criminalization, procedural forces, jurisdiction, international collaboration, and network access supplier duty and obligation are pivotal to forestall and combat cybercrime. Insightful measures, purview, electronic proof and global collaboration can give the genuinely necessary maintain toward this path. It was found out that the private sector was armed against cyber-attacks and uses digital protection development yet various little and medium-sized associations erroneously observe they won't be a goal and don't figure out how to guarantee their frameworks [1]. A few organizations have found a way to counter cybercrime acts, including using lawful action. Internet specialist co-ops and facilitating suppliers can assume a vital function in finding the culprits behind these attacks. They have tools that can be used to save data and crime analysis in order to explore crime; help clients to recognize traded off PCs; block a few sorts of illegal substance, for example, spam; and by and large help a protected interchanges climate for their clients. Academic institutions speak to a significant accomplice in cybercrime anticipation through information improvement and sharing; legislation and strategy advancement; the improvement of innovation and specialized guidelines; the conveyance of

[1]Syed Mohd Uzair Iqbal, Cyber-crimes & cyber-terrorism in India, UNIVERSITY (2013), http://shodhganga.inflibnet.ac.in:8080/jspui/handle/10603/63591 (last visited Nov 25, 2023)

specialized help; and cooperation with law approval specialists. For fruitful digital wrongdoing evasion practices, fitting sanctioning, reasonable organization, headway of criminal equity and law execution cutoff, guidance and care, the improvement of a strong data bases,& co-operation across govt, networks, private areas in the public & global circles are required.

a) Judicial approach on Cyber Crime and Cyber Terrorism

The Bank NSP Case [2] For this circumstance an organization student of a bank got the married. It was found out that the messages exchanged between the couples were through the office systems only later they steered some attention about their marriage and created some fake email addresses. for instance, "Indian bar affiliations" and started sending mails to their clients impersonating themselves to be officials. These were done within the bank systems. Lather they lost their clients started getting complaints about the bank's efficiency Unfortunately the bank was held questionable for the messages sent under their authority.

b) Avnish Bajaj versus State (2008)

"In December 2004 the Chief Executive Officer of Bazee.com was caught considering the way that he was selling a limited plate (CD) with unfriendly material on the site, and even Disk was furthermore conjointly sold-out in the market of Delhi. The Delhi police and thusly the Mumbai police investigated the issue together ut after some time the CEO was let free on bail."

c) State versus Navjot Sandhu @ Afsan master (2004)

"The Bureau of Police Research and Development, Hyderabad had dealt with this case. A framework was recovered from the manipulator who attacked the Parliament. The framework which was kept from the two dread-based oppressors, who were gunned down on thirteenth December 2001 when the Parliament was enduring an onslaught, was sent off Computer Criminology Division of BPRD. The framework contained a couple of confirmations that demanded the two manipulator's manners of thinking, dominatingly the sticker of the Ministry of the made a fake ID with fake Indian administration seal which was made in jammu and Kashmir."

d) Andhra Pradesh State Road versus Income-Tax Officer (1961)

The person owned a plastic firm and caught with huge amount of money which was found out to be unaccountable money by the vigilance officers. The owner had submitted around 6000 duplicates documents showing legitimacy of the trade that he carried out but they found out that all these documents were fabricated once the deal was set between his agents. The owner tried pretend that he was looking out 5 companies when he only was running one company with the help of fake internet tools which framed and tampered these transactions of bargins and extra expenditure accordingly to their wish for which he was held liable and caught by the vigilant officers.

e) CBI versus Arif Azim (2003)

This was India's first case relating to cyber-crime conviction. The case where sony runs new site under the name of Sony India pvt ltd which allowed NRI to transfer and sell sony products to any people they want in India, the money transactions were also made through the website. In 2002, somebody got a deal under the name of Arif Azim who lived in Noida, she also shared her transaction details and MasterCard passwords. Later the things were sold under the guidance of Arif. These transactions and transfers were being recorded. But later there was issues rising where the visa authority refused to accept the things and denied its entry. It was found that it was a foul play where Arif Azim charged with web cheating under section IPC sections 418,419 and 420. the convicts were caught by the police and investigated his whole connections in Noida and his access of the website. "In this issue, the CBI had confirmation to exhibit their case so the accused yielded his fault. The court condemned Arif Azim under Section 418, 419 and Section 420 of the IPC, this being the first occasion when that a cybercrime case has been condemned. The court, felt that since the disputant was a child of 24 years and a first-time convict, a thoughtful view ought to have been taken. As such, the court delivered the respondent on the probation for one year."

f) Harsh Sharma v. The State of Maharashtra

certain individuals were accused for theft of data and programming from their chief and charged under segments 408 and 420 of the IPC and besides under segments 43, 65 and 66 of the IT Act. These segments, other than section408 of the IPC, have been analyzed already. Section408 of the IPC oversees criminal infiltrate of trust by associate or laborer and states that "whoever, being a delegate or specialist or used as a specialist or specialist, and being in any capacity enriched in such cutoff with property, or with any space over property, completes criminal break of trust in respect of that property, will be repulsed with restriction of one or the other depiction for a term which may contact seven years, and will comparably be perpetrated to fine

Conclusion

The determination and recommendations of an exploration work showed up at after finish of all sections covering various tops of the theory is certifiably not a solid one. They are, as a rule, layered one, for example coming about of the sedimentation, all things considered. It is here exceptional to express that in an exploration work it is unimaginable to expect to continue with unhampered contentions in the majority of the conditions. Subsequently, these ends and entries should likewise be perused related to ends toward the finish of each part. We as a whole realize that change is an all-inclusive marvel of the nature and change is inescapable and the predicament that progression in innovation can't be stayed away from, likely, ICT insurgency occurred which made the virtual universe of cyberspace appear. Innovations of PC, Internet, cellphone, TV and so on have fortified the IT area. Out of these the Internet is the main development. The expansion of ICT and its different appearance for example the Internet, PC, cell telephone, satellites and so forth have transformed ourselves in diverse manner. No circle of our life can escape from the impact of IT insurgency. The assembly of registering, the Web and correspondence and outstanding improvement of cutting-

[2] Chinmayi Arun, Gatekeeper Liability and Article 19(1)(A) of the Constitution of India, SSRN ELECTRONIC JOURNAL (2015), http://www.ssrn.com/abstract=2643278 (last visited Nov 26, 2023)

edge advancement have conveyed epic preferences yet with these new points of interest come more genuine risks both from locally similarly as across borders. The new open entryways made in the internet have updated the constraint of individual liable gatherings and criminal associations that have emerged to abuse shortcomings in the internet, thus, cybercrimes have arisen. These new types of bloodless crimes are currently presenting difficulties against people, society, government and worldwide associations. In the time of data innovation insurgency when banking, administration, correspondence, transportation, protection and so on are being managed through the cyberspace, the quick advancement of the Internet network and its function in the rise of data age have constrained public governments and global organizations to address the requirement for guideline and wellbeing of the data expressways. Presently the Internet has made the world borderless so crimes done by the psychological oppressors in the cyber space draw in the consideration of the world. Cyberspace is presently being utilized as paradise by the cyber fear mongers; enormous psychological militant associations are utilizing data advancements, where they can choose targets and sorts of weapon and can finish their arrangements of assault in actual world as well as in virtual world also. Cyber terrorism is unique in relation to the traditional crimes so the law requirement organizations find vulnerable to check it inside the current structure of infrastructural instrument. Under these conditions it's about time that when everyone need to consider the threat associated with the data thruway. It has seen that the Internet offers fear based oppressors unrivaled chances. Various sorts of cybercrime in their own specific manner present various difficulties to legitimate requirement offices and governments. These reach from crimes against people to genuine crimes perpetrated against the State. Cyberspace, similar to some other social space where people cooperate, speaks to a space that can't be isolated from the actual world, where methods of conduct have created inside certain connections that have developed, for as far back as 200 years in a world arrangement of country states. The web difficulties the observation of sealed public outskirts that can be policed and controlled by country states. Without a doubt the limit of computer interchanges to sidestep lawful and state experts on the size of the web is presumably phenomenal throughout the entire existence of interchanges. In spite of the fact that the exact degree of unlawful lead including the utilization of PCs is muddled, the quick development of the web and internet business has focused on such unlawful lead for administrators, policymakers, industry, and law implementation offices. Similarly, as authentic use of the web is developing, so too is the web progressively being utilized to encourage customary offenses. Cybercrime is the deadliest pandemic facing earth in this thousand year. A cyber-criminal can pulverize sites and entries by hacking and planting infections, convey out online fakes by moving assets starting with one comer of the globe then onto the next, gain admittance to exceptionally secret and delicate data, cause provocation by email dangers or profane material, play charge cheats, enjoy cyber sexual entertainment including youngsters, and perpetrate multitudinous different crimes on the web. Hence it is said that none is secure in the cyber world.

References

1. Sarmah A, *et al*. A brief study on Cyber Crime and Cyber Law's of India. 04.
2. Mittal S, Singh A. A Study of Cyber Crime and Perpetration of Cyber Crime in India. 2014;171-186.
3. Monisha TRH, Rajan MS. An Analytical Study on Offences under IT Act with Special Reference to Section 66. 18.
4. Andhra Pradesh State Road v. Income-Tax Officer, Hyderabad. 14 Mar 1961. Available from: https://indiankanoon.org/doc/620068/ (last visited Nov 20, 2023).
5. Bajaj Avnish v. State. 29 May 2008. Available from: https://indiankanoon.org/doc/309722/ (last visited Nov 20, 2024).
6. National Crime Records Bureau. Crime in India Table Contents. Available from: https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?field_date_value%5Bvalue%5D%5Byear%5D=2016&field_select_table_title_of_crim_value=20&items_per_page=50 (last visited Nov 20, 2024).
7. Hello Counsel. Cyber Crime & IT Law Cases in India. Available from: http://www.hellocounsel.com/cyber-crime/ (last visited Nov 19, 2023).
8. Kaushik RD. Cyber-crime in India: A critical study in modern perspective. 2013. Available from: http://shodhganga.inflibnet.ac.in:8080/jspui/handle/10603/189479 (last visited Nov 19, 2023).
9. Mondaq. Cyber Crimes under the IPC and IT Act - An Uneasy Co-existence. Available from: https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence (last visited Nov 21, 2023).
10. Arun C. Gatekeeper Liability and Article 19(1)(A) of the Constitution of India. SSRN Electronic Journal. 2015. Available from: http://www.ssrn.com/abstract=2643278 (last visited Nov 21, 2023).
11. History of computer crime. 705-721.
12. Cabrera E, McArdle R. The Evolution of Cybercrime and Cyberdefense. 35.
13. Singh T. Success in any field of human activity leads to crime that need. 15.